The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
02/14/2012

SUBJECT:
Vulnerability in C Run-Time Library Could Allow Remote Code Execution (MS12-013)

OVERVIEW:
A vulnerability has been discovered in the C Run-Time Library which could allow an attacker to take complete control of an affected system. The C Run-Time Library is a collection of support files used to implement basic functions such as input/output and memory management. The vulnerability can be exploited if a user visits or is redirected to a malicious web page, or runs a specially crafted media file hosted on a website or sent as an email attachment.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
Microsoft Windows Vista SP2
Microsoft Server 2008 R2 SP1
Microsoft Server 2008 SP2
Microsoft Windows 7 SP1

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in the Microsoft C Run-Time Library which could allow an attacker to take complete control of an affected system. Specifically, the 'msvcrt' dynamic link library (DLL) incorrectly calculates the size of a buffer in memory, resulting in an overflow condition. In order to leverage this vulnerability, an attacker would need to convince a user to open a specially crafted media file, either hosted on a website or sent as an email attachment.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms12-013

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0150

Security Focus:
http://www.securityfocus.com/bid/51913